What is Claimed:

1. A system that manages the partitioning of an application comprising:

a base layer that hosts the operation of a first environment and a second environment, the application comprising:

a first software object that executes in said first environment, said first software object handling a plurality of data and including logic to identify a first of said plurality of data as not processable by said software object; and

a second software object that executes in said second environment and that processes said first of said plurality of data in a manner that resists tampering with said first of said plurality of data,

said base layer comprising or hosting logic that receives said first of said plurality of data from said software object and routes said first of said plurality of data to said second environment.

2. The system of claim 1, wherein said first software object causes a representation of said first of said plurality of data to be displayed on a display device, said representation comprising one or more indecipherable tokens.

3. The system of claim 2, wherein said one or more indecipherable tokens are either: (1) the same size as each other, or (2) of sizes that are unrelated to the content of said first of said plurality of data.

4. The system of claim 1, and wherein the resistance to tampering provided by said second software object comprises said second environment resisting interference with the display of said first of said plurality of data by writing a representation of said first of said plurality of data into a video memory associated with a display device so as to cause said representation to supersede any image at a location on said display device at which said representation is to be displayed.

5. The system of claim 1, wherein said first of said plurality of said is entered on a keyboard, and wherein the resistant to tampering provided by said second software object comprises resisting

tampering with said first of said plurality of data in transit from said keyboard to an input stream of said second software object.

6. The system of claim 5, wherein said second application signs said first of said plurality of data to prevent subsequent tampering with said first of said plurality of data.

7. The system of claim 6, wherein said second environment signs said first of said plurality of data and the signature created by said second application as an indication that said first of said plurality of data and said signature were created in said second environment.

8. The system of claim 1, wherein said base layer comprises a component that assigns a first identifier to said second environment.

9. The system of claim 8, wherein said first of said plurality of data includes, or is accompanied by, said first identifier and a second identifier that identifies said second software object.

10. The system of claim 1, wherein said first environment is associated with a first specification that describes the behavior of said first environment, wherein said second environment is associated with a second specification that describes the behavior of said second environment, wherein there is a higher level of assurance that said second environment will conform to said second specification than that said first environment will conform to said first specification.

11. The system of claim 10, wherein said second software object relies upon the behavior of the second environment in order to resist tampering with said first of said plurality of data.

12. The system of claim 1, wherein said base layer is said second environment, or is included within said second environment.

13. A method of a first software object, which executes in a first environment, handling data to which a policy applies, the method comprising:

the first software object encountering the data;

the first software object determining that the data is not processable by the first software object;

the first software object causing the data to be provided to a second software object that executes in a second environment that provides a first level of assurance that actions performed in the second environment will be performed correctly, wherein the second software object processes the data in a manner that uses said assurance to resist tampering with the data by acts arising outside of the second environment.

14. The method of claim 13, wherein the resistance to tampering comprises a resistance to a change in said data.

15. The method of claim 14, wherein said data is to be displayed on a visual display device, and wherein the resistance to tampering comprises displaying a representation of said data in a location on said visual display device and superseding any image other than said representation that is rendered at said location.

16. The method of claim 13, wherein said first software object causes a representation of the data to be displayed on a visual display device, said representation comprising one or more indecipherable tokens.

17. The method of claim 16, wherein said representation are either: (1) the same size as each other, or (2) of sizes that are unrelated to the content of said first of said plurality of data.

18. The method of claim 16, wherein said first software object or said second software object, or a combination of said first software object and said second software object, cause items displayed on said visual display device to be changed in at least one respect to permit viewing of an image of the data produced by said second software object.

19. The method of claim 14, wherein said data is provided using a keyboard, and wherein the resistance to tampering comprises resisting a change to the data in transit from the keyboard to the input stream of the second software object.

20. The method of claim 13, wherein said security policy specifies that said data is to be handled by said second software object.

21. The method of claim 13, wherein said data includes, or is associated with, a first label that identifies said second environment as a location in which said data is to be processed.

22. The method of claim 21, wherein said data includes, or is associated with, a second label that identifies said second software object as a processor for said data, and wherein said second environment routes said data to said second software object based on said second label.

23. The method of claim 13, wherein said second environment is associated with a first specification that describes the behavior of said second environment, and wherein said assurance provides that said second environment will conform to said specification.

24. The method of claim 13, wherein said first environment is associated with a second specification that describes the behavior of said first environment, and wherein said first environment provides a second level of assurance that actions performed in the first environment will be performed correctly, said second level of assurance being relatively lower than said first level of assurance.

25. A computer-readable medium having encoded thereon code and data to allow a user to operate on first and second classes of data, said second class of data requiring a relatively higher level of protection from tampering than said first class of data, said code and data comprising:

a first software object associated with a first specification that describes the behavior of said first software object, said first software object comprising instructions to:

operate on members of said first class of data;

recognize a member of said second class of data as not being processable by

said first software object; and

cause said member of said second class of data to be routed to a second software object; and

said second software object, which is associated with a second specification that describes the behavior of said second software object, there being a relatively higher level of assurance that said second software object will conform to said second specification than that said first software object will conform to said first specification, said second software object comprising instructions to operate on members of said second class of data.

26. The computer-readable medium of claim 25, wherein said first software object operates in a first environment, wherein said second software object operates in a second environment, wherein said first environment is associated with a third specification that describes the behavior of said first software environment, wherein said second environment is associated with a fourth specification that describes the behavior of said second environment, wherein the level of assurance that said second environment will conform to said fourth specification is relatively higher than the level of assurance that said first environment will conform to said first specification, and wherein the assurance that said second software object will conform to said second specification derives from said second software object's reliance on the behavior of the second environment.

27. The computer-readable medium of claim 25, wherein each member of said second class of data comprises: (1) a first label indicating that said member of said second class is to be processed in said second environment, and (2) a second label assigned by said second environment indicating that said member of said second class is to be processed by said second software object.

28. The computer-readable medium of claim 27, wherein said first software object causes said member of the second class to be routed to said second software object by sending said member of the second class to a base component, said first label being assigned by said base component, said second label being recognizable by said second environment and not by said base component.

29. The computer-readable medium of claim 25, wherein said first software object displays output on a visual display device, said output including one or more locations on said visual display device in which said member of said second class is to be displayed, and wherein said second software object displays a representation of said data of said second class in said one or more locations.

30. The computer-readable medium of claim 29, wherein said representation is displayed in said one or more locations by said second environment causing said representation to be written into a video memory associated with said visual display device.

31. The computer-readable medium of claim 25, wherein said member of said second class comprises data to be entered using a keyboard, and wherein causing said member of said second class of data to be routed to said second software object comprises said second environment transporting said member of said second class from said keyboard to said second software object in a manner that resists tampering with said member of said second class by events arising outside of said second environment.

32. A system that supports the partitioning of an application into at least a first software object and a second software object, the system hosting a first environment and a second environment, the first software object running in the first environment, the second software object running in the second environment, the system comprising an application programming interface that exposes at least one of the following methods:

a first method that receives from the first software object a first data object that comprises: (1) data processable by the second software object, and (2) a first identifier assigned by the system to the second environment; and that routes said first data object to said second environment based on said first identifier;

a second method that creates a second data object that comprises: (1) data processable by the second software object; (2) said first identifier; (3) authentication data that allows a subsequent determination that said second data object has not been tampered with since being created by said second method;

a third method that receives, from the first environment, a second identifier associated with the second software object, and that directs that an instance of the second software object be created; and

a fourth method that receives, from the first software environment: (1) a third data object, and (2) a third identifier associated with said first software object, and that directs that an instance of said first software object be created based on having received said third identifier, and that directs that said first software object operate on said third data object.

33. The system of claim 32, wherein said first environment is associated with a first specification that describes the behavior of said first environment, wherein said second environment is associated with a second specification that describes the behavior of said second environment, wherein there is a first level of assurance that said first environment will conform to said first specification, wherein there is a second level of assurance that said second environment will conform to said second specification, and wherein said second level of assurance is relatively higher than said first level of assurance.

34. The system of claim 33, wherein said second software provides assurance that said second software object will protect data, said assurance being provided at least in part by relying on the behavior of the second environment.